المقدمة

تم إصدار **مخطط الشبكة "Network Mapper"** (**Nmap**) في الأصل بواسطة *Gordon Fyodor Lyon* في مجلة *phrack* المجلد 7 عدد 51. تعتبر اليوم واحدة من أفضل الأدوات لاستطلاع الشبكة والتدقيق الأمني في مجال أمن المعلومات. تم تقديم الإصدار العام الأول كماسح متقدم للمنافذ إلى جانب ورقة تصف البحث حول تقنيات اكتشاف المنافذ، لكنها أصبحت أكثر من ذلك بكثير. لقد تطورت إلى أداة أساسية ومميزة بالكامل تتضمن العديد من المشاريع الفرعية الرائعة الأخرى، مثل: Ncrack و Ncat و Nping و Zenmap و Nmap Scripting Engine (جميعها متاحة على https://nmap.org). توصف Nmap على النحو التالي في الموقع الرسمي:

"*Network Mapper*) *Nmap*) هي أداة مجانية ومفتوحة المصدر لاكتشاف الشبكة والتدقيق الأمني. كما يجد العديد من مسؤولي الشبكة والأنظمة أنها مفيدة لمهام مثل مخزون الشبكة وإدارة جداول ترقية الخدمة ومراقبة المضيف أو وقت تشغيل الخدمة، يستخدم Nmap حزم IP الأولية بطرق جديدة لتحديد المضيفات المتوفرة على الشبكة، والخدمات (اسم التطبيق وإصداره) التي يقدمها هؤلاء المضيفون، وأنظمة التشغيل (وإصدارات نظام التشغيل) التي يقومون بتشغيلها، ونوع عوامل تصفية الحزم/جدران الحماية قيد الاستخدام، والعديد من الخصائص الأخرى. تم تصميمها لفحص الشبكات الكبيرة بسرعة، ولكنها تعمل بشكل جيد ضد المضيفين الفرديين. يعمل Nmap على جميع أنظمة تشغيل الحاسوب الرئيسية، وتتوفر الحزم الثنائية الرسمية لأنظمة Linux و Windows و Mac OS X."

تم إنشاء أدوات أخرى في المشروع لتلبية الاحتياجات المحددة للمستخدمين. *Nping* (https://nmap.org/nping/) متخصص في إنشاء حزم الشبكة. يركز *Ncrack* (https://nmap.org/ncrack/) على تكسير مصادقة الشبكة. *Ncat* (https://nmap.org/ncat/) هو إصدار محسّن من Netcat ويسمح للمستخدمين بقراءة بيانات الشبكة وكتابتها وإعادة توجيهها وتعديلها. *Zenmap* (https://nmap.org/zenmap/) عبارة عن واجهة

مستخدم رسومية عبر الأنظمة الأساسية تركز على سهولة الاستخدام. أخيرًا، يأخذ *Nmap Scripting Engine* (https://nmap.org/book/nse.html) المعلومات الممسوحة التي تم الحصول عليها من الأهداف ويوفر واجهة للمستخدمين لكتابة مهام إضافية.

مجتمع Nmap نشط جدًا، لذلك أشجعك دائمًا على مواكبة الإصدارات وأحدث التصحيحات. تتم الإعلانات والمناقشات في القائمة البريدية للتطوير، لذلك إذا كنت ترغب في المساهمة في المشروع، أوصيك بالاشتراك فيه.

هذا الفصل الأول للقادمين الجدد. بدءًا من بناء Nmap، سوف نكون على دراية بجميع أدوات مشروع Nmap. في عدد قليل من الوصفات، ستتعلم مدى مرونة Nmap وفعاليتها حقًا، ولكن بينما نتحرك عبر الفصول، سنتعمق في المكونات الداخلية لتعلم ليس فقط كيفية استخدام الأدوات ولكن لتوسيعها وإنشاء الخاصة بك. ستساعدك المهام العملية المختارة لهذا الفصل على بصمات الأصابع للأنظمة المحلية والبعيدة، وخرائط الشبكات، وصياغة حزم الشبكات المخصصة، وحتى تحديد الأنظمة التي تحتوي على كلمات مرور ضعيفة.

كود المصدري لـ Nmap

خلال الوصفات التالية، سنستخدم الأدوات المضمنة في مشروع Nmap، لذا من الأفضل تثبيت أحدث الإصدارات الآن. ستوضح هذه الوصفة كيفية تنزيل أحدث نسخة من كود المصدر من مستودعات التطوير وتثبيت Nmap والأدوات ذات الصلة في نظامك القائم على UNIX.

نحن نفضل دائمًا العمل مع أحدث إصدار ثابت من المستودع لأن الحزم المجمعة مسبقًا تستغرق وقتًا في التحضير وقد يفوتنا تصحيح أو نص NSE جديد. ستوضح الوصفة التالية عملية تكوين وبناء وصيانة نسخة محدثة من مشروع Nmap في ترسانتك.

استعد

قبل المتابعة، يجب أن يكون لديك اتصال إنترنت فعال والوصول إلى عميل التخريب "subversion". تأتي الأنظمة الأساسية المستندة إلى Unix مع عميل سطر أوامر يسمى **(svn) subversion**. للتحقق مما إذا كان مثبتاً بالفعل في النظام الخاص بك، فقط افتح المحطة واكتب الأمر التالي:

```
$ svn
```

إذا لم يتم العثور على الأمر، فقم بتثبيت svn باستخدام مدير الحزم المفضل لديك أو قم ببنائه من الكود المصدري. إن التعليمات الخاصة بإنشاء svn من الكود المصدري خارج نطاق هذا الكتاب، ولكن يتم توثيقها على الإنترنت على نطاق واسع. استخدم محرك البحث المفضل لديك للعثور على تعليمات محددة لنظامك.

عند إنشاء Nmap، سنحتاج أيضًا إلى مكتبات إضافية مثل تعريفات التطوير من **OpenSSL** أو الأمر make. في الأنظمة المستندة على دبيان، جرب الأمر التالي لتثبيت التبعيات المفقودة:

```
#apt-get install libssl-dev autoconf make g++
```

لاحظ أن OpenSSL اختياري، ويمكن بناء Nmap بدونه؛ ومع ذلك، سيتم تعطيل Nmap؛ لأنه يستخدم OpenSSL للوظائف المتعلقة بالأعدادات الصحيحة متعددة الدقة، والتجزئة والتشفير/فك التشفير لاكتشاف الخدمة، ومحرك Nmap Scripting Engine.

كيف افعلها...

1. أولاً، نحتاج إلى الحصول على نسخة من الكود المصدري من المستودعات الرسمية. لتنزيل أحدث إصدار من فرع التطوير، نستخدم الأمر *checkout* (أو *co*):

```
$svn co --username guest https://svn.nmap.org/nmap
```

2. الآن يجب أن تشاهد قائمة الملفات التي تم تنزيلها والرسالة سحب المراجعة <رقم المراجعة>. مجلد جديد يحتوي على كود المصدر متاح الآن في مجلد العمل الخاص بك. بعد تثبيت التبعيات المطلوبة، نكون على استعداد لتجميع Nmap مع الإجراء القياسي: تكوين وإنشاء وإجراء التثبيت "*configure, make,* and *make install*". انتقل إلى المجلد الذي يحتوي على الكود المصدري وأدخل ما يلي:

```
$./configure
```

3. إذا اكتملت عملية التكوين بنجاح، فيجب أن ترى بعض فن ASCII اللطيف (يتم اختياره عشوائيًا، لذلك قد لا ترى هذا بالضرورة):



لتجميع Nmap، استخدم `make`:

$make

الآن يجب أن تشاهد nmap الثنائية في مجلد العمل الحالي الخاص بك. أخيرًا، لتثبيت Nmap على النظام، قم بتنفيذ `make install` مع امتيازات إدارية:

```
#make install
```

يجب أن ترى رسالة : NMAP SUCCESFULLY INSTALLED عند اكتمال العملية.

كيف يعمل...

يحتوي مستودع SVN المستضاف على https://svn.nmap.org/nmap على أحدث إصدار مستقر من Nmap ولديه وصول عالمي للقراءة يتيح لأي شخص الحصول على نسخة من كود المصدر. قمنا ببناء المشروع من الصفر للحصول على أحدث التصحيحات والميزات. كما قامت عملية التثبيت الموضحة في هذه الوصفة بتثبيت Zenmap و Ndiff و Nping.

هناك المزيد...

تشبه عملية تجميع Nmap تجميع التطبيقات الأخرى المستندة إلى Unix، ولكن هناك العديد من متغيرات الوقت المترجمة التي يمكن تعديلها لتكوين التثبيت. يوصى باستخدام ثنائيات الملفات المسبقة للمستخدمين الذين لا يمكنهم ترجمة Nmap من المصدر. يوصى بأنظمة مستندة إلى Unix بسبب بعض قيود Windows الموضحة في https://nmap.org/book/inst-windows.html.

الفروع التجريبية

إذا كنت ترغب في تجربة أحدث إبداعات فريق التطوير، فهناك مجلد باسم nmap-exp يحتوي على العديد من الفروع التجريبية للمشروع. الكود المخزن في هذا المجلد غير مضمون للعمل طوال الوقت حيث يتم استخدامه كصندوق رمل "sandbox" حتى يصبح جاهزاً للدمج في الإنتاج. عنوان URL الفرعي لهذا المجلد هو https://svn.nmap.org/nmap-exp.

تحديث نسخة العمل المحلية الخاصة بك

مشروع Nmap نشط جدًا (خاصة خلال فصل الصيف)، لذلك لا تنس تحديث نسختك بانتظام. إذا احتفظت بنسخة عاملة من مستودع svn، فيمكنك القيام بذلك بسهولة بتنفيذ الأوامر التالية داخل هذا المجلد:

```
$svn up
$make
#make install
```

تخصيص عملية البناء

إذا كنت لا تحتاج إلى أدوات Nmap الأخرى، مثل: Nping أو Ndiff أو Zenmap، فيمكنك استخدام توجيهات تكوين مختلفة لحذف التثبيت أثناء خطوة التكوين:

```
./configure --without-ndiff
./configure --without-zenmap
./configure --without-nping
```

للحصول على قائمة كاملة بتوجيهات التكوين، استخدم معلمة الأمر `help--`:

```
$./configure --help
```

الحزم سابقة التجهيز

يمكن العثور على حزم Nmap مسبقة التجهيز لجميع الأنظمة الأساسية الرئيسية على https://nmap.org/download.html لأولئك الذين لا يستطيعون الوصول إلى مترجم. عند العمل مع حزم سابقة التجهيز، تأكد فقط من الحصول على إصدار حديث إلى حد ما لتجنب فقدان التحسينات أو الإصلاحات المهمة.

العثور على مضيفات نشطة في شبكتك

يعد العثور على مضيفات مباشرة في شبكتك المحلية مهمة شائعة بين مختبري الاختراق ومسؤولي النظام لتعداد الأجهزة النشطة في جزء الشبكة. يوفر Nmap معدلات اكتشاف أعلى من أداة ping التقليدية؛ لأنها ترسل تحقيقات إضافية من طلبات ICMP echo التقليدي لاكتشاف المضيفين.

تصف هذه الوصفة كيفية إجراء فحص ping باستخدام Nmap للعثور على مضيفات مباشرة في شبكة محلية.

كيف أفعل ذلك؟

افتح الطرفية واكتب الأمر التالي: V1

$ nmap -sP 192.168.1.1/24

قم بتشغيل مسح ping على مقطع شبكة باستخدام الأمر التالي: V2

#**nmap -sn <target>**

تظهر النتيجة المضيفين المتصلين بالإنترنت وقد استجابوا لمسح ping.

```
Nmap scan report for 192.168.1.102
Host is up.
Nmap scan report for 192.168.1.254
Host is up (0.0027s latency).
MAC Address: 5C:4C:A9:F2:DC:7C (Huawei Device Co.)
```

```
Nmap done: 256 IP addresses (2 hosts up) scanned in 10.18 seconds
```

في هذه الحالة، وجدنا مضيفين متصلين بالشبكة. عثر Nmap أيضًا على عنوان MAC، وحدد مورد جهاز التوجيه المنزلي.

كيف تعمل...

يستخدم Nmap خيار sP- لمسح ping. هذا النوع من الفحص مفيد جدًا في تعداد المضيفين في الشبكة. يستخدم حزمة TCP ACK وطلب ICMP echo إذا تم تنفيذه كمستخدم جذر، أو حزمة SYN مرسلة عبر syscall ()connect إذا تم تشغيلها من قبل مستخدمين لا يمكنهم إرسال حزم خام "raw packets".

يستخدم CIDR/24 في 192.168.1.1/24 للإشارة إلى أننا نريد مسح جميع عناوين IP 256 في شبكتنا.

هناك المزيد...

يتم استخدام طلبات ARP عند مسح شبكة Ethernet محلية كمستخدم مميز، ولكن يمكنك تجاوز هذا السلوك من خلال تضمين خيار send-ip--.

nmap -sP --send-ip 192.168.1.1/24

traceroute

استخدم traceroute-- لتضمين مسار بين جهازك وكل مضيف تم العثور عليه.

```
Nmap scan report for 192.168.1.101
Host is up (0.062s latency).
MAC Address: 00:23:76:CD:C5:BE (HTC)

TRACEROUTE
HOP RTT      ADDRESS
1   61.70 ms 192.168.1.101

Nmap scan report for 192.168.1.102
Host is up.

Nmap scan report for 192.168.1.254
Host is up (0.0044s latency).
MAC Address: 5C:4C:A9:F2:DC:7C (Huawei Device Co.)

TRACEROUTE
HOP RTT     ADDRESS
1   4.40 ms 192.168.1.254

Nmap done: 256 IP addresses (3 hosts up) scanned in 10.03 seconds
```

NSE SCRIPTS

لا يقوم فحص Ping بفحص المنفذ أو الكشف عن الخدمة، ولكن يمكن تمكين Nmap Scripting Engine للبرامج النصية اعتماداً على قواعد المضيف، مثل حالات الكشف عن الشم و dns-brute،

```
# nmap -sP --script discovery 192.168.1.1/24

Pre-scan script results:
| broadcast-ping:
|_  Use the newtargets script-arg to add the results as targets
Nmap scan report for 192.168.1.102
Host is up.

Host script results:
|_dns-brute: Can't guess domain of "192.168.1.102"; use dns-brute.domain script argument.

Nmap scan report for 192.168.1.254
Host is up (0.0023s latency).
MAC Address: 5C:4C:A9:F2:DC:7C (Huawei Device Co.)

Host script results:
|_dns-brute: Can't guess domain of "192.168.1.254"; use dns-brute.domain script argument.
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 256 IP addresses (2 hosts up) scanned in 14.11 seconds
```

المسح باستخدام نطاقات منافذ محددة

هناك حالات عندما يبحث مسؤول النظام عن الأجهزة المصابة التي تستخدم منفذًا معينًا للتواصل، أو عندما يبحث المستخدمون فقط عن خدمة معينة أو منفذ مفتوح ولا يهتمون بالباقي. يؤدي تضييق نطاقات المنافذ المستخدمة أيضًا إلى تحسين الأداء، وهو أمر مهم جدًا عند مسح أهداف متعددة.

يوضح هذا الشرح كيفية استخدام نطاقات المنافذ عند إجراء مسح Nmap.

كيف أفعلها؟

افتح الطرفية واكتب الأمر التالي:

nmap -p80 192.168.1.1/24

ستظهر قائمة بالمضيفين مع حالة المنفذ 80 في النتائج.

كيف يعمل؟

يستخدم Nmap خيار p- لتعيين نطاقات المنافذ المراد مسحها. يمكن دمج هذا الخيار مع أي طريقة مسح. في المثال السابق، استخدمنا المدخل p80- للإشارة إلى Nmap بأننا مهتمون فقط بالمنفذ 80.

يستخدم CIDR/24 في 192.168.1.1/24 للإشارة إلى أننا نريد مسح جميع عناوين IP 256 الموجودة في شبكتنا.

هناك المزيد ...

هناك العديد من التنسيقات المقبولة لخيار p مدخلات:

- قائمة منافذ

nmap -p80,443 localhost

- نطاق منافذ

nmap -p1-100 localhost

- كل المنافذ

nmap -p- localhost

- منافذ محددة بواسطة البروتوكولات

nmap -pT:25,U:53 <target>

- باسم الخدمة

nmap -p smtp <target>

- باسم الخدمة مع حروف التوسعة (wildcards)

nmap -p smtp* <target>

- فقط الخدمات المسجلة في nmap

nmap -p[1-65535] <target>